AMENDMENTS TO THE CLAIMS

1-18. (Cancelled)

19. (Previously Presented) Apparatus for ensuring the integrity of an application executed on a computer having data storage arranged sectorwise, comprising:

apparatus for learning about the normal access behavior of said application to said data storage arranged sectorwise by monitoring accesses of said application to elements of said data storage during a limited period; and

an enforcement device, operative after said period is over, for identifying and preventing said application from accessing elements of data storage that do not correspond with the normal behavior of said application.

20. (Cancelled)

21. (Previously Presented) Apparatus according to claim 19 wherein said enforcement device is operative to prompt a user to give specific permission, upon occurrence of an attempt of the program to access files not accessed during said learning period.

22. (Previously Presented) Apparatus for ensuring the integrity of computer applications to be run in association with a computer having data storage arranged sectorwise in a storage device, comprising:

apparatus for assigning a general enforcement file to each new program;

apparatus for learning about the program by monitoring instances of user permission given to the program's attempts to make file accesses during a learning period; and

an enforcement device operative, after said learning period is over, to treat attempts of the program to access files to which the user permitted access during said learning period more leniently than attempts of the program to access files to which the user did not permit access during said learning period.

23. (Previously Presented) Apparatus according to claim 19 wherein said enforcement device is based at least partly on instances of specific permission being given by the user to the program to access certain files, wherein the enforcement device treats attempts of the program to access files to which the user permitted access during said learning period more leniently than attempts of the program to access files to which the user did not permit access during said learning period.

24. (Currently Amended) Apparatus for ensuring the integrity of a computer application to be run in association with a computer having data storage arranged sectorwise in a storage device, comprising:

apparatus for assigning a general enforcement file to each new program;

apparatus for learning about the program by monitoring the program's attempts to make file accesses during a learning period; and

an enforcement device operative, after said learning period is over, to treat attempts of the program to access files accessed during said learning period more leniently than attempts of the program to access files not accessed during said learning period, said enforcement device being ~~is~~ based at least on instances of specific permission being given by the user to said application to access locations of said data storage, wherein said enforcement device treats attempts of said application to access locations of said data storage to which the user has permitted ~~to~~ access during said learning period more leniently than attempts of the program to access files to which the user did not permit access during said learning period.

25. (Previously Presented) A method for detecting abnormal behavior of a first application executed on a computer system, and preventing the damage thereupon, comprising:

monitoring accesses of said application to elements of data storage arranged sectorwise in a storage device over a period of time and storing information about said accesses in an enforcement file, thereby learning the normal behavior of said application; and

when said period is over, detecting attempts of said application to access

elements of data storage that do not correspond to said normal behavior as determined by said enforcement file and inhibiting said accesses, thereby preventing the damage thereupon.

26. (Previously Presented) A method according to claim 25, further comprising enabling the user of said first application to determine said normal behavior during said learning period.

27. (Previously Presented) A method according to claim 25, further comprising enabling the user of said first application to determine said normal behavior after said learning period is over.

28. (Previously Presented) A method according to claim 26, further comprising enabling the user of said first application to determine said normal behavior after said learning period is over.

29. (Previously Presented) A method according to claim 25, further comprising detecting attempts of a daughter application of said first application to access elements of data storage that do not correspond to said normal behavior as determined by said enforcement file and inhibiting said accesses, thereby preventing the damage thereupon.

30. (Previously Presented) A method according to claim 26, further comprising detecting attempts of a daughter application of said first application to access elements of data storage that do not correspond to said normal behavior as determined by said enforcement file and inhibiting said accesses, thereby preventing the damage thereupon.

31. (Previously Presented) A method according to claim 27, further comprising detecting attempts of a daughter application of said first application to access elements of data storage that do not correspond to said normal behavior as determined by said enforcement file and inhibiting said accesses, thereby preventing the damage thereupon.

32. (Previously Presented) A method according to claim 25, further comprising detecting attempts of a second application to access elements of data storage that do not correspond to said normal behavior as determined by said enforcement file and inhibiting said accesses, thereby preventing the damage thereupon.

33. (Previously Presented) A method according to claim 26, further comprising detecting attempts of a second application to access elements of data storage that do not correspond to said normal behavior as determined by said enforcement file and inhibiting said accesses, thereby preventing the damage thereupon.

34. (Previously Presented) A method according to claim 27, further comprising detecting attempts of a second application to access elements of data storage that do not correspond to said normal behavior as determined by said enforcement file and inhibiting said accesses, thereby preventing the damage thereupon.

35. (Previously Presented) A method according to claim 29, wherein said second application is executed on a second computer.

36. (Previously Presented) The apparatus of claim 19, wherein only normal accesses of said application to elements of said data storage are monitored during said limited time period.

37. (Previously Presented) The apparatus of claim 22, wherein said apparatus for learning about the program is for learning about only the normal access behavior of the program during said learning period.

38. (Previously Presented) The apparatus of claim 24, wherein said apparatus for learning about the program is for learning about only the normal access behavior of the program during said learning period.

39. (Currently Amended) A method according to ~~The apparatus of~~ claim 25, wherein said

monitoring of said accesses of said application to elements of data storage learns only the normal behavior of said application.

40. (New) Apparatus for ensuring the integrity of an application executed on a computer having data storage arranged sectorwise, comprising:

apparatus for learning about the normal access behavior of said application to said data storage arranged sectorwise by monitoring accesses of said application to elements of said data storage during a limited period; and

an enforcement device, operative after said period is over, for granting said application no access rights to any elements of data storage other than those elements accessed during said limited period, to which access will be allowed.

41. (New) A method for detecting abnormal behavior of a first application executed on a computer system, and preventing the damage thereupon, comprising:

monitoring accesses of said application to elements of data storage arranged sectorwise in a storage device over a limited period of time and storing information about said accesses in an enforcement file, thereby learning the normal behavior of said application; and

when said period is over, granting said application no access rights to any elements of data storage other than those elements accessed during said limited period, to which access will be allowed.

42. (New) A method for ensuring normal access behavior of a program, the method comprising the steps of:

providing a list of access permissions of said program to elements of data storage;

monitoring access requests of said program to data storage; and

upon indicating a request to access an element of data storage which does not comply with said list, blocking said attempt.

43. (New) A method according to claim 42, further comprising:

during a limited period in which said program is assumed to be uninfected by a virus, upon indicating by said monitoring a request to access an element of data storage which is not on said list, adding said element to said list as allowable for access.

44. (New) A method according to claim 42, wherein said monitoring further includes requests of a daughter application of said program to access data storage.